(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 663 108 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
13.11.2013 Bulletin 2013/46

(51) Int Cl.:
H04W 12/02 *(2009.01)*

(21) Application number: **13002458.1**

(22) Date of filing: **08.05.2013**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **10.05.2012 US 201213468263**

(71) Applicant: **Telefonaktiebolaget L M Ericsson (Publ)**
164 83 Stockholm (SE)

(72) Inventor: **Gauthier, Claude**
Quebec, J3L 3T7 (CA)

(74) Representative: **Röthinger, Rainer et al**
Wuesthoff & Wuesthoff
Patent- und Rechtsanwälte
Schweigerstrasse 2
81541 München (DE)

(54) Identifying a wireless device of a target user for communication interception based on individual usage pattern(s)

(57) Systems and methods for intercepting communications in a cellular communication network are disclosed. In one embodiment, one or more individual usage patterns are detected for a target user based on usage data collected from a known wireless device of the target user. The one or more individual usage patterns for the target user are compared to usage data collected from other wireless devices to identify another wireless device that has usage data that matches the one or more individual usage patterns for the target user to at least a predefined threshold degree. In response, one or more predefined actions are taken with respect to the matching wireless device. In one embodiment, an authorized authority is notified of the matching wireless device and/or communications to and/or from the matching wireless device are automatically intercepted and delivered to the authorized authority

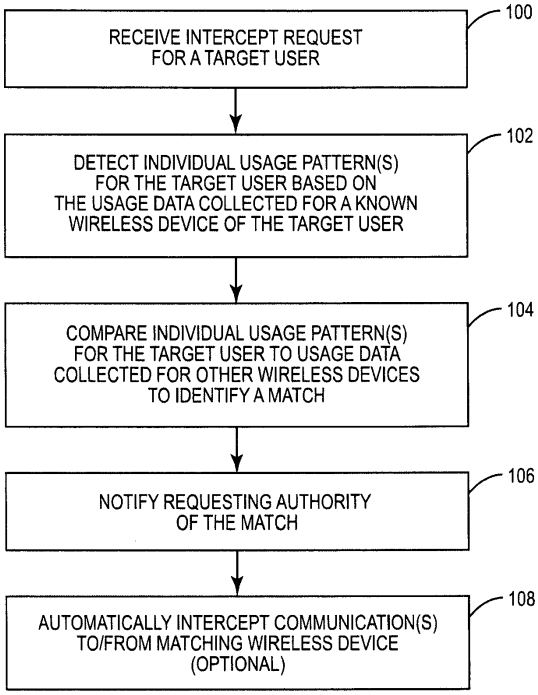

FIG. 2

EP 2 663 108 A1

Description

Field of the Disclosure

[0001] The present disclosure relates to intercepting communications in a cellular communication network.

Background

[0002] Authorized authorities (e.g., law enforcement agencies) often intercept communications, such as calls, made in cellular communication networks in order to monitor the content of communications to and from target users such as members of gang organizations, members of the mafia, drug dealers, etc. As such, cellular communication networks are required to have the appropriate infrastructure to permit interception of communications to and from target users. However, these target users often use multiple wireless devices (e.g., multiple mobile phones) and frequently change wireless devices in order to thwart the authorized authorities from intercepting their communications. Further, these wireless devices are often registered in the names of different individuals. As an example, a target user may switch mobile phones every four or five weeks, where each mobile phone may be registered in the name of a different individual. When the target user switches to a new mobile phone, the authorized authorities are no longer able to intercept calls to and from the target user on the new mobile phone. Thus, there is a need for a system and method for intercepting communications to and from a target user even if the target user uses multiple mobile phones and/or switches to different mobile phones.

Summary

[0003] Systems and methods for intercepting communications in a cellular communication network are disclosed. In one embodiment, one or more individual usage patterns are detected for a target user based on usage data collected from a known wireless device of the target user. The usage data collected from the known wireless device of the target user includes, but is not limited to, location information that defines a location of the known wireless device of the target user, accelerometer information from an accelerometer of the known wireless device of the target user, gyroscope information from a gyroscope of the known wireless device of the target user, electronic compass information from an electronic compass of the known wireless device of the target user, application usage information for one or more applications executed on the known wireless device of the target user, game usage information for one or more games executed on the known wireless device of the target user, web browsing information for one or more web browsers executed on the known wireless device of the target user, calling patterns on the known wireless device of the target user, texting patterns on the known wireless device of the target user, or any combination thereof. The one or more individual usage patterns for the target user are compared to usage data collected from other wireless devices to identify another wireless device that has usage data that matches the one or more individual usage patterns for the target user to at least a predefined threshold degree. In response, one or more predefined actions are taken with respect to the matching wireless device. In one embodiment, an authorized authority is notified of the matching wireless device and/or communications to and/or from the matching wireless device are automatically intercepted and delivered to the authorized authority.

[0004] Those skilled in the art will appreciate the scope of the present disclosure and realize additional aspects thereof after reading the following detailed description of the preferred embodiments in association with the accompanying drawing figures.

Brief Description of the Drawing Figures

[0005] The accompanying drawing figures incorporated in and forming a part of this specification illustrate several aspects of the disclosure, and together with the description serve to explain the principles of the disclosure.

Figure 1 illustrates a system for intercepting communications to and from a target user in a cellular communication network according to one embodiment of the present disclosure; and

Figure 2 is a flow chart that illustrates a process for identifying a new or additional wireless device or a potential new or additional wireless device of a target user based on one or more individual usage patterns for the target user detected based on usage data collected from a known wireless device of the target user according to one embodiment of the present disclosure.

Detailed Description

[0006] The embodiments set forth below represent the necessary information to enable those skilled in the art to practice the embodiments and illustrate the best mode of practicing the embodiments. Upon reading the following description in light of the accompanying drawing figures, those skilled in the art will understand the concepts of the disclosure and will recognize applications of these concepts not particularly addressed herein. It should be understood that these concepts and applications fall within the scope of the disclosure and the accompanying claims.

[0007] Figure 1 illustrates a cellular communication system 10 that includes a communication intercept system 12 that utilizes individual usage patterns to identify wireless devices that are being used by target users ac-

cording to one embodiment of the present disclosure. As used herein, a "target user" is a user for which communications are to be intercepted by the communication intercept system 12. As illustrated, the cellular communication system 10 includes the communication intercept system 12 and a cellular communication network 14. The cellular communication network 14 generally operates to provide cellular communication service to a number of wireless devices 16-1 through 16-N. The wireless devices 16-1 through 16-N are generally referred to herein collectively as wireless devices 16 and individually as wireless device 16. The cellular communication network 14 is any type of cellular communication network such as, for example, a 3G or 4G cellular communication network. Each of the wireless devices 16 is any type of wireless device served by the cellular communication network 14 such as, for example, a mobile phone, a tablet computer equipped with a cellular network interface, or the like.

[0008] The communication intercept system 12 operates to intercept communications to and from target users at the request of a requesting authority 18. The requesting authority 18 may be, for example, a law enforcement agency, but is not limited thereto. More generally, the requesting authority 18 is any individual or entity having legal authority to intercept communications to and from one or more particular users, which are referred to herein as target users. In this particular embodiment, the communication intercept system 12 includes an administration function 20 and a delivery function 22. The administration function 20 operates to receive an intercept request from the requesting authority 18 that identifies a target user 24 for which interception is desired. The intercept request includes information that identifies a known wireless device of the target user 24, which in this example is the wireless device 16-1. In some embodiments, the administration function 20 also verifies that the requesting authority 18 is legally authorized to intercept communications to and from the target user 24 by, for example, requiring that the requesting authority 18 provide a valid warrant to intercept communications to and from the target user 24.

[0009] Upon receiving and, in some embodiments, verifying the intercept request, the administration function 20 sends an intercept request to one or more Intercept Control Elements (ICEs) 26 in the cellular communication network 14. The intercept request includes information that identifies the known wireless device of the target user 24, which again in this example is the wireless device 16-1. The ICEs 26 are generally network nodes in the cellular communication network 14 that enable interception of communications to and from target users such as the target user 24. For example, for a 3G cellular communication network, the ICEs 26 may be 3G Mobile Service Mobile Switching Center (MSC) servers, 3G Gateway MSC servers, Serving General Packet Radio Service (GPRS) Support Nodes (SGSNs), or Gateway GSNs (GGSNs). As another example, for a 4G cellular communication network and in particular a Long Term Evolution (LTE) or LTE-Advanced cellular communication network, the ICEs 26 may be eNodeB, Mobility Management Entity (MME), Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), or Home Subscriber Server (HSS).

[0010] In response to the intercept request from the administration function 20 of the communication intercept system 12, the ICEs 26 intercept communications to and from the wireless device 16-1 of the target user 24 and return corresponding intercept data to the delivery function 22 of the communication intercept system 12. The delivery function 22 then returns the intercept data to the requesting authority 18. The intercept data may include, for example, the content of a call to or from the wireless device 16-1 of the target user 24.

[0011] In order to detect other wireless devices 16 used by the target user 24, the communication intercept system 12 also includes a data collection function 28, a usage pattern detection function 30, and a matching function 32. The data collection function 28 operates to collect usage data from the wireless devices 16-1 through 16-N and store the usage data in a usage data repository 34. Notably, the wireless devices 16-1 through 16-N may be all wireless devices served by the cellular communication network 14 or a subset of all wireless devices served by the cellular communication network 14. In this example, the data collection function 28 collects the usage data via the ICEs 26, but is not limited thereto. For each wireless device 16, the data collection function 28 collects one or more of the following: location information that defines a geographic location of the wireless device 16 (e.g., Global Positioning System (GPS) data including latitude and longitude data), gyroscope output data from a gyroscope of the wireless device 16, accelerometer output data from an accelerometer of the wireless device 16, electronic compass output data from an electronic compass of the wireless device 16, application usage information regarding use of applications executed on the wireless device 16 by the corresponding user, game usage information regarding use of games executed on the wireless device 16 by the corresponding user, web browsing information regarding web browsing activities of the corresponding user, a call log for calls made and/or received by the wireless device 16, a text messaging log for texts sent and/or received by the wireless device 16, or any combination thereof.

[0012] More specifically, the location information includes information that defines geographic locations at which the wireless device 16 has been located and preferably corresponding timestamps that define dates and/or times of day that the wireless device 16 was located at those geographic locations. The geographic locations of the wireless device 16 may be expressed using any two-dimensional or three-dimensional representation such as, for example, latitude, longitude, and potentially altitude obtained from a GPS receiver of the wireless device 16, street address, point of interest (e.g., Walmart Store #12345). The gyroscope output data preferably in-

cludes readings output from a gyroscope of the wireless device 16 that define an orientation of the wireless device 16 and, preferably, corresponding timestamps for those readings. The accelerometer output data preferably includes readings output from an accelerometer of the wireless device 16 and corresponding timestamps for those readings. The electronic compass output data preferably includes readings output from an electronic compass that define a direction in which the wireless device 16 is pointing.

[0013] The application usage data generally defines applications used by a user of the wireless device 16 and preferably timing information that defines dates and/or times of day that those applications were used by the user. For example, the application usage data may include data that indicates that the user used an email application executing on the wireless device 16 from 7:30am to 8:00am on Wednesday April 11, 2012. In a similar manner, the application usage data may include similar data for other uses of the email application and/or other applications executing on the wireless device 16. In a similar manner, the game usage data generally defines games played by the user on the wireless device 16 and preferably corresponding timing information that defines dates and/or times at which the user played those games. The web browsing information generally includes information that defines web browsing activities of the user of the wireless device 16 and preferably timing information for those web browsing activities. The web browsing activities may include, for example, visiting a website, logging into a web-based service (e.g., a social networking website, a banking website, or the like), or logging out of a web-based service.

[0014] The call log generally includes information that identifies calls made and/or received by the wireless device 16. In one embodiment, the call log includes a list of phone numbers called by the wireless device 16 and, potentially, corresponding timestamps for the calls. Lastly, the texting log generally includes information that identifies other devices to which texts were sent by the wireless device 16 or from which texts were received by the wireless device 16. In one embodiment, the texting log includes a list of phone numbers to which texts were sent and/or from which texts were received and corresponding timestamps that indicate dates and times at which those texts were sent/received.

[0015] The usage pattern detection function 30 generally operates to detect usage patterns for target users, such as the target user 24, based on the usage data collected for known wireless devices of the target users and store those individual usage patterns for the target user 24 in a usage patterns repository 36. In one embodiment, in response to receiving an intercept request from the requesting authority 18 and, depending on the particular embodiment, verifying the intercept request, the administration function 20 notifies the usage pattern detection function 30 of a target user and a known wireless device of the target user subject to the intercept request. Using the target user 24 as an example, the usage pattern detection function 30 then processes the usage data collected from the wireless device 16-1 (i.e., the known wireless device of the target user 24) to detect one or more individual usage patterns for the target user 24 using any suitable pattern detection algorithm. The usage pattern detection function 30 may process usage data collected from the wireless device 16-1 collected prior to and/or after the intercept request to detect the one or more individual usage patterns for the target user 24. Further, the amount of usage data processed may vary. For instance, the amount of usage data may be all usage data collected from the wireless device 16-1 or only usage data collected from the wireless device 16-1 over several days, weeks, months, or longer prior to and/or after receiving the receiving the intercept request for the target user 24.

[0016] In general, the individual usage patterns detected for the target user 24 may be any type of usage pattern that can be detected based on the usage data collected from the wireless device 16-1. For example, the usage pattern detection function 30 may detect a location-based usage pattern that is a pattern of geographic locations visited by the target user 24 and, in some embodiments, times of the day and/or day(s) of the week that the target user 24 visits those geographic locations. As another example, the usage pattern detection function 30 may detect a gyroscope-based usage pattern that is a pattern of movement of the wireless device 16-1 and, in some embodiments, times of the day and/or day(s) of the week that the target user 24 makes those movements. In addition or alternatively, the gyroscope-based usage pattern may include information that identifies triggering events for the movements in the pattern (e.g., the target user 24 typically moves the wireless device 16-1 in a particular manner in response to receiving a call and typically moves the wireless device 16-1 in a different manner in response to receiving a text message). In a similar manner, an accelerometer-based usage pattern or an electronic compass based usage pattern may be detected.

[0017] As yet another example, the usage pattern detection function 30 may detect a pattern of usage for one or more applications executing on the wireless device 16-1. This pattern of usage of the application(s) may indicate, for example, time(s) of the day, day(s) of the week, and/or geographic location(s) at which the target user 24 uses the application(s). In a similar manner, the usage pattern detection function 30 may detect a game usage pattern for one or more games on the wireless device 16-1. The game usage pattern may indicate time(s) of the day, day(s) of the week, and/or geographic location (s) at which the target user 24 plays one or more games.

[0018] As a yet another example, the usage pattern detection function 30 may detect a pattern of usage of a web browser of the wireless device 16-1. The pattern of usage of the web browser may indicate time(s) of the day, day(s) of the week, and/or geographic location(s) at

which the target user 24 uses the web browser and/or visits particular website(s). The pattern of usage of the web browser may additionally or alternatively indicate patterns for other web-based activities such as logging into particular websites, logging off particular websites, posting on particular blogs, or the like.

[0019] As a final example, the usage pattern detection function 30 may detect a pattern of phone calls and/or text messages for the wireless device 16-1. The pattern of phone calls and/or text messages may, for example, identify phone numbers called/texted from the wireless device 16-1 and, potentially, time(s) of the day, day(s) of the week, and/or geographical location(s) at which the target user 24 calls and/or texts those phone numbers. Similarly, the pattern of phone calls and/or text messages may, for example, identify phone numbers that call and/or text the target user 24 and, potentially, time(s) of the day, day(s) of the week, and/or geographical location(s) at which the target user 24 receives calls and/or texts from those phone numbers.

[0020] The matching function 32 generally operates to compare the usage data collected by the data collection function 28 and stored in the usage data repository 34 to the individual usage patterns of the target users stored in the usage patterns repository 36. When the usage data collected from one of the wireless devices 16 matches the one or more individual usage patterns of a target user, then that wireless device is identified as a wireless device, or potential wireless device, of the target user. Using the target user 24 as an example, assume that the target user 24 switches to wireless device 16-2 as illustrated in Figure 1. After a sufficient amount of usage data is collected from the wireless device 16-2, the matching function 32 will detect that the usage data collected from the wireless device 16-2 matches the one or more usage patterns of the target user 24 stored in the usage patterns repository 36. The wireless device 16-2 is then identified as a wireless device or a potential wireless device of the target user 24. In this particular embodiment, the matching function 32 sends an indication of the match to the delivery function 22, which in turn notifies the requesting authority 18 that the wireless device 16-2 has been identified as a wireless device or a potential wireless device of the target user 24. In addition or alternatively, the communication intercept system 12 may then automatically begin interception of communications to and from the target user 24 on the wireless device 16-2.

[0021] Figure 2 is a flow chart that illustrates the operation of the communication intercept system 12 of Figure 1 to identify a new or additional wireless device or a potential new or additional wireless device of the target user 24 according to one embodiment of the present disclosure. First, the communication intercept system 12, and specifically the administration function 20, receives an intercept request from the requesting authority 18 to intercept communications to and from the target user 24 (step 100). In response, the usage pattern detection function 30 then detects one or more individual usage patterns for the target user 24 based on usage data collected from a known wireless device of the target user 24, which for this discussion is the wireless device 16-1 (step 102). The one or more individual usage patterns for the target user 24 are stored in the usage patterns repository 36. The matching function 32 compares the one or more individual usage patterns for the target user 24 to usage data collected from the other wireless devices 16 (i.e., the wireless devices 16 other than the known wireless device 16-1 of the target user 24) to identify one of the other wireless devices 16 having usage data that matches the one or more individual usage patterns of the target user 24 to at least a predefined threshold degree (step 104). The predetermined threshold degree may be defined in any suitable manner. For example, the predefined threshold degree may specified as a percentage (e.g., 25%, 50%, or 75%) such that the individual usage patterns of the target user 24 and the usage data of the other wireless device must match to at least that percentage before a match is identified.

[0022] In this example, the wireless device 16-2 is identified as having usage data that matches the one or more individual usage patterns of the target user 24 to at least the predefined threshold degree. In response, the communication intercept system 12 notifies the requesting authority 18 of the match (step 106). In one embodiment, the communication intercept system 12 notifies the requesting authority 18 of the wireless device 16-2 and the degree of match between the one or more individual usage patterns of the target user 24 and the usage data of the wireless device 16-2. In another embodiment, the communication intercept system 12 notifies the requesting authority 18 that the wireless device 16-2 has been identified as a potential new or additional wireless device of the target user 24 if the match is greater than a first predefined threshold degree and less than a second predefined threshold degree that is greater than the first predefined threshold degree and notifies the requesting authority 18 that the wireless device 16-2 is a new or additional wireless device of the target user 24 if the match is greater than the second predefined threshold degree.

[0023] Optionally, the communication intercept system 12 automatically begins interception of communications to and from the target user 24 at the wireless device 16-2 having usage data that sufficiently matches the one or more individual usage patterns of the target user 24 (step 108). In one embodiment, the communication intercept system 12 automatically begins interception of communication to and from the target user 24 at the wireless device 16-2 in response to identifying the match in step 104.

[0024] However, in another embodiment, a second higher threshold degree of match may be required before automatically beginning interception of communications to and from the target user 24 at the wireless device 16-2. In an alternative embodiment, the communication intercept system 12 begins interception of communications to and from the target user 24 at the wireless device 16-2

only after sending the notification in step 106 and then receiving an intercept request from the requesting authority 18 for the target user 24 at the wireless device 16-2.

[0025] The communication intercept system 12 described herein is implemented in hardware or more preferably a combination of hardware and software. For example, the communication intercept system 12 may be implemented as a server computer that executes appropriate software. Such software is stored on a non-transitory computer-readable. Further, the communication intercept system 12 may be implemented on a single hardware node (e.g., a single server computer) or be distributed among multiple hardware nodes (e.g., distributed over multiple server computers).

[0026] The following acronyms are used throughout this disclosure.

- GGSN Gateway General Packet Radio Service Support Node
- GPRS General Packet Radio Service
- GPS Global Positioning System
- HSS Home Subscriber Server
- ICE Intercept Control Element
- LTE Long Term Evolution
- MME Mobility Management Entity
- MSC Mobile Switching Center
- P-GW Packet Data Network Gateway
- SGSN Serving General Packet Radio Service Support Node
- S-GW Serving Gateway

[0027] Those skilled in the art will recognize improvements and modifications to the preferred embodiments of the present disclosure. All such improvements and modifications are considered within the scope of the concepts disclosed herein and the claims that follow.

Claims

1. A method of operation of a communication intercept system associated with a cellular communication network, comprising:

   detecting one or more individual usage patterns for a target user based on usage data collected from a known wireless device of the target user served by the cellular communication network;

   comparing the one or more individual usage patterns for the target user to usage data collected from a plurality of other wireless devices served by the cellular communication network to identify a wireless device from the plurality of other wireless devices that has usage data that matches the one or more individual usage patterns of the target user to at least a predefined threshold degree; and

   taking one or more predefined actions with respect to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree.

2. The method of claim 1 wherein at least one of the one or more individual usage patterns of the target user is based on one or more of, and in particular at least two of:

   - location information collected from the known wireless device of the target user, wherein the location information optionally comprises latitude and longitude data;
   - gyroscope information collected from the known wireless device of the target user;
   - electronic compass information collected from the known wireless device of the target user;
   - accelerometer information collected from the known wireless device of the target user;
   - application usage information collected from the known wireless device of the target user;
   - game usage information collected from the known wireless device of the target user;
   - web browsing information collected from the known wireless device of the target user;
   - a call log for the known wireless device of the target user; and
   - a text messaging log for the known wireless device of the target user.

3. The method of any of the preceding claims wherein taking the one or more predefined actions comprises notifying an authorized authority of the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree.

4. The method of any of the preceding claims wherein taking the one or more predefined actions comprises automatically intercepting at least one of a group consisting of: communications from the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications from the target user and communications to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications to the target user.

5. The method of any of the preceding claims wherein taking the one or more predefined actions comprises:

   notifying an authorized authority of the wireless device that has usage data that matches the one

or more individual usage patterns of the target user to at least the predefined threshold degree; and

automatically intercepting at least one of a group consisting of: communications from the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications from the target user and communications to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications to the target user.

6. The method of any of the preceding claims wherein taking the one or more predefined actions comprises:

notifying an authorized authority of the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree; and

if the usage data of the wireless device matches the one or more individual usage patterns of the target user to at least a second predefined threshold degree that is greater than the predefined threshold degree, automatically intercepting at least one of a group consisting of: communications from the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications from the target user and communications to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications to the target user.

7. The method of any of the preceding claims further comprising:

collecting the usage data from the known wireless device of the target user; and

collecting the usage data from the plurality of other wireless devices.

8. The method of any of the preceding claims wherein the plurality of other wireless devices is all other wireless devices served by the cellular communication network.

9. The method of any of the preceding claims wherein the plurality of other wireless devices is a subset of all other wireless devices served by the cellular communication network.

10. A communication intercept system associated with a cellular communication network, comprising:

one or more first communication interferences configured to enable communication between the communication intercept system and an authorized authority;

one or more second communication interfaces configured to enable the communication between the communication intercept system and the cellular communication network; and

a processing sub-system associated with the one or more first communication interfaces and the one or more second communication interfaces that is configured to:

receive a communication intercept request for a target user from the authorized authority via the one or more first communication interfaces;

collect, via the one or more second communication interfaces, usage data from a known wireless device of the target user served by the cellular communication network;

detect one or more individual usage patterns for the target user based on the usage data collected from the known wireless device of the target user;

collect, via the one or more second communication interfaces, usage data from a plurality of other wireless devices served by the cellular communication network;

compare the one or more individual usage patterns for the target user to the usage data collected from the plurality of other wireless devices to identify a wireless device from the plurality of other wireless devices that has usage data that matches the one or more individual usage patterns of the target user to at least a predefined threshold degree; and

take one or more predefined actions with respect to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree.

11. The communication intercept system of claim 10 wherein at least one of the one or more individual usage patterns of the target user is based on one or more of, and in particular at least two of:

- location information collected from the known wireless device of the target user, wherein the location information optionally comprises latitude and longitude data;
- gyroscope information collected from the

known wireless device of the target user;
- accelerometer information collected from the known wireless device of the target user;
- electronic compass information collected from the known wireless device of the target user;
- application usage information collected from the known wireless device of the target user;
- game usage information collected from the known wireless device of the target user;
- web browsing information collected from the known wireless device of the target user;
- a call log for the known wireless device of the target user; and
- a text messaging log for the known wireless device of the target user.

12. The communication intercept system of claim 10 or 11 wherein the one or more predefined actions comprise notifying the authorized authority of the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree.

13. The communication intercept system of any of claims 10 to 12 wherein the one or more predefined actions comprise automatically intercepting at least one of a group consisting of: communications from the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications from the target user and communications to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications to the target user.

14. The communication intercept system of any of claims 10 to 13 wherein the one or more predefined actions comprise:

notifying the authorized authority of the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree; and

automatically intercepting at least one of a group consisting of: communications from the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications from the target user and communications to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications to the target user.

15. The communication intercept system of any of claims 10 to 14 wherein the one or more predefined actions comprise:

notifying the authorized authority of the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree; and

if the usage data of the wireless device matches the one or more individual usage patterns of the target user to at least a second predefined threshold degree that is greater than the predefined threshold degree, automatically intercepting at least one of a group consisting of: communications from the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications from the target user and communications to the wireless device that has usage data that matches the one or more individual usage patterns of the target user to at least the predefined threshold degree as communications to the target user.

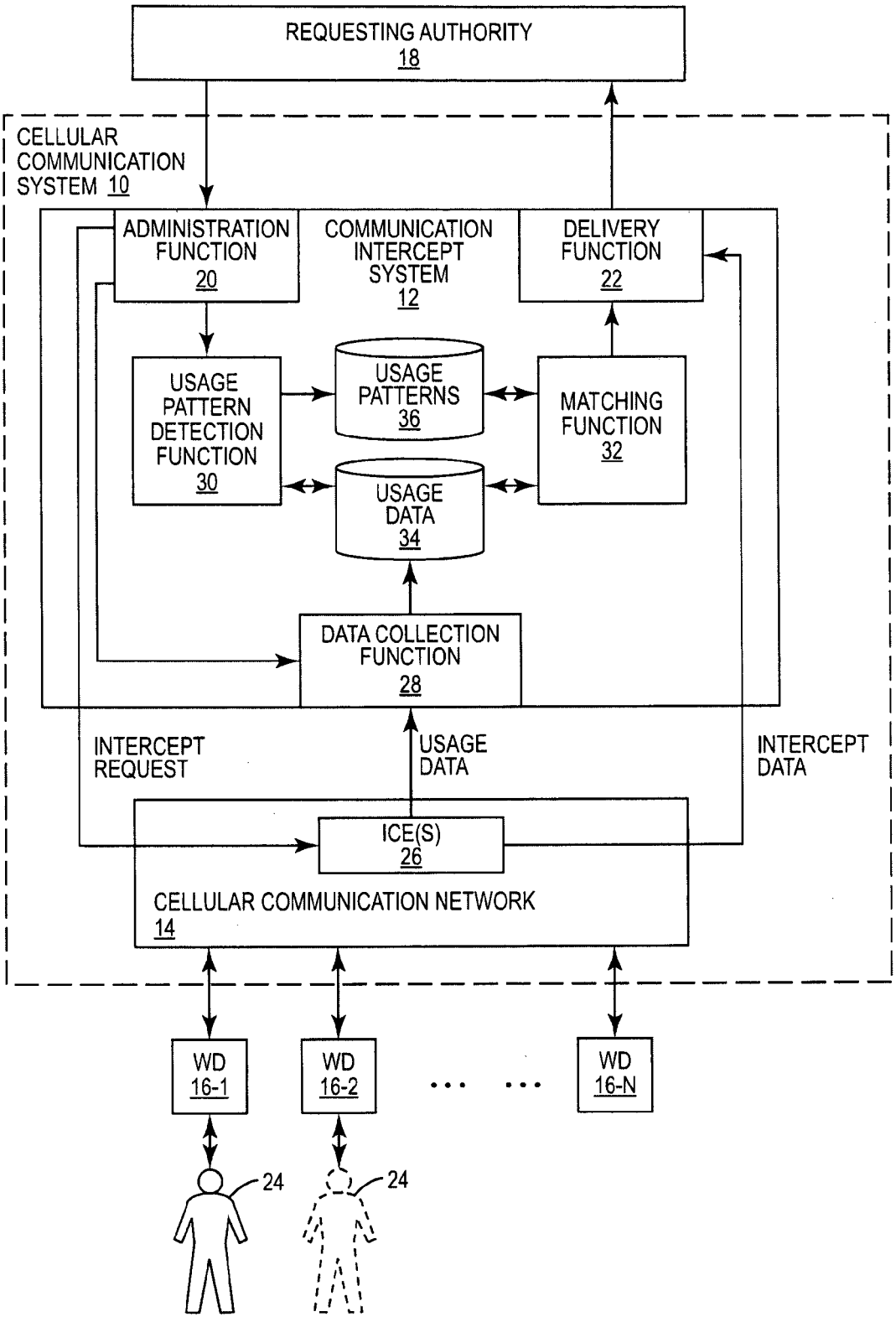
REQUESTING AUTHORITY
18
CELLULAR COMMUNICATION SYSTEM 10
ADMINISTRATION FUNCTION
20
COMMUNICATION INTERCEPT SYSTEM
12
DELIVERY FUNCTION
22
USAGE PATTERN DETECTION FUNCTION
30
USAGE PATTERNS
36
MATCHING FUNCTION
32
USAGE DATA
34
DATA COLLECTION FUNCTION
28
INTERCEPT REQUEST
USAGE DATA
INTERCEPT DATA
ICE(S)
26
CELLULAR COMMUNICATION NETWORK
14
WD 16-1
WD 16-2
WD 16-N
24
24

FIG. 1

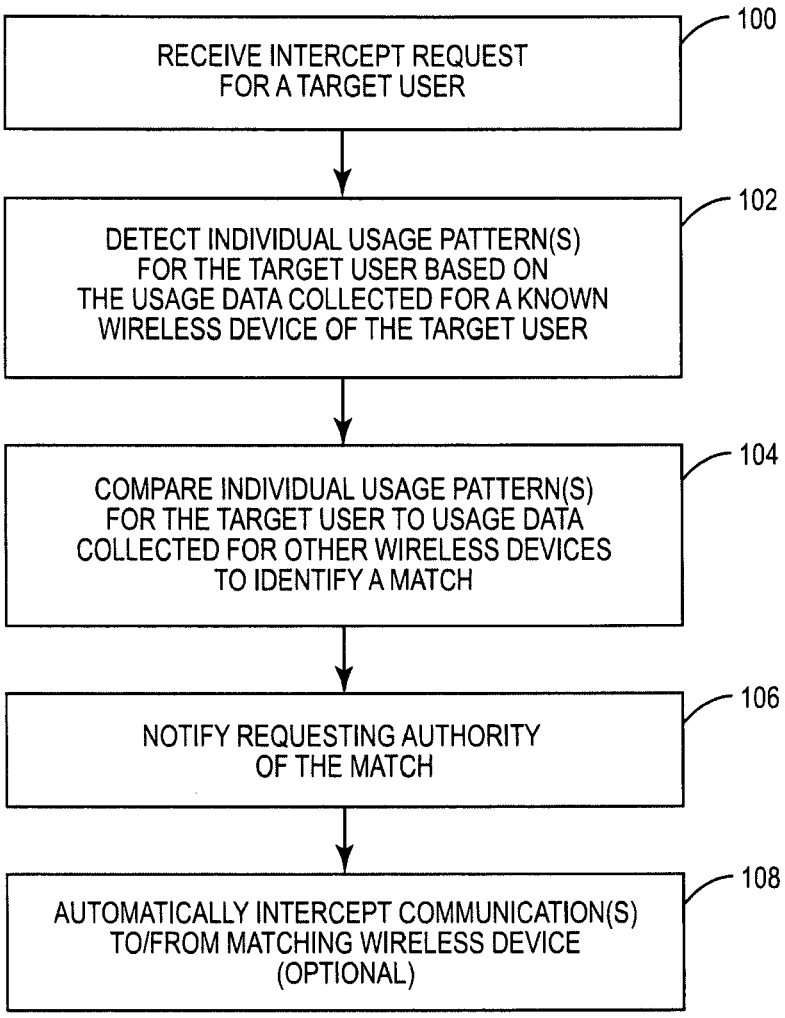
RECEIVE INTERCEPT REQUEST FOR A TARGET USER
100
DETECT INDIVIDUAL USAGE PATTERN(S) FOR THE TARGET USER BASED ON THE USAGE DATA COLLECTED FOR A KNOWN WIRELESS DEVICE OF THE TARGET USER
102
COMPARE INDIVIDUAL USAGE PATTERN(S) FOR THE TARGET USER TO USAGE DATA COLLECTED FOR OTHER WIRELESS DEVICES TO IDENTIFY A MATCH
104
NOTIFY REQUESTING AUTHORITY OF THE MATCH
106
AUTOMATICALLY INTERCEPT COMMUNICATION(S) TO/FROM MATCHING WIRELESS DEVICE (OPTIONAL)
108

FIG. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 13 00 2458

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 2 169 992 A1 (ALCATEL LUCENT [FR]) 31 March 2010 (2010-03-31) * abstract * * paragraph [0001] - paragraph [0006] * * paragraph [0009] * * paragraph [0023] - paragraph [0024] * * paragraph [0049] - paragraph [0051] * * paragraph [0063] * -----	1-15	INV. H04W12/02
X	CA 2 500 082 A1 (DEMELLO AARON [CA]; MILLER ALEXANDER [CA]) 18 September 2006 (2006-09-18) * abstract * * page 11, line 16 - line 32 * * page 15, line 15 - line 30 * * page page 8, line 1 - line 9 * -----	1-15	
X	US 2012/072453 A1 (GUERRA LISA [US] ET AL) 22 March 2012 (2012-03-22) * paragraph [0022] - paragraph [0023] * * paragraph [0036] - paragraph [0043] * * paragraph [0050] - paragraph [0054] * * paragraph [0068] - paragraph [0069] * -----	1-15	TECHNICAL FIELDS SEARCHED (IPC) H04L H04W H04M
X	US 2008/162397 A1 (ZALTZMAN ORI [IL]) 3 July 2008 (2008-07-03) * abstract * * paragraph [0014] - paragraph [0015] * -----	1-15	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	5 September 2013	Lamelas Polo, Yvan

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

1 EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 13 00 2458

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-09-2013

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2169992 A1	31-03-2010	EP 2169992 A1	31-03-2010
		FR 2936670 A1	02-04-2010
CA 2500082 A1	18-09-2006	NONE	
US 2012072453 A1	22-03-2012	NONE	
US 2008162397 A1	03-07-2008	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82